REMARKS

Claims 1-30, 31 and 33 are pending in the present application. Claims 32 and 34 were canceled previously, and Claims 1-2, 20-21, and 31 are amended herein.

Applicants filed a Response to Office Action with the USPTO, in regard to the present application, on October 14, 2004. Remarks and comments in such Response are incorporated herein by reference.

I. 35 U.S.C. § 102, Anticipation

The Examiner has rejected Claims 1-7, 10-17, 20-26, and 29-30 under 35 U.S.C. § 102 as being anticipated by U.S. Patent No. 5,966,705 to Koneru et al. This rejection is respectfully traversed.

II. 35 U.S.C. § 103, Obviousness

The Examiner has rejected claims 8-9, 18-19, 27-28, 31 and 33 under 35 U.S.C. § 103 as being obvious in view of Koneru et al., in combination with U.S. Patent No. 6,092,196 to Reiche.

III. Response to Rejection of Claim 1

In making their invention, as stated in the application at page 5, lines 11-12, Applicants were concerned with communication between a web client and a web site having both secure and non-secure web pages. Applicants recognized that for web sites such as e-commerce web sites, it is necessary to allow for authentication and session management when holding a conversation with a web client. As is well known to those of skill in the art, cookies are a popular method for session management between a web site and a web client. Cookie based session management must incorporate a secure communication protocol, to prevent unauthorized users from stealing sensitive data contained in the cookie. One such protocol is HTTPS (HTTP/SSL). These conclusions of Applicants are set forth in the present application, such as at page 1, lines 24-25, page 2, lines 22-23 and page 3, lines 17-19.

As stated in the application at page 5, lines 1-6, Applicants recognized further that there are significant problems in switching between a secure protocol such as HTTPS and a non-secure protocol such as HTTP, while using a single cookie. For example, switching between HTTPS and HTTP can be troublesome in that when a web client logs on to a web site using HTTPS, a cookie is issued to authenticate the web client. However, if the web client later browses a non-secure page at the web site using HTTP, the same cookie is sent to the web client in clear text. At this point an unauthorized user can steal the cookie. Thus, using a single cookie in this situation, particularly when a user is continually switching between secure and non-secure web pages, can jeopardize the security of the web site.

Applicants overcome the above drawbacks and disadvantages of the prior art by means of their invention, which provides that both different cookies and different protocols are to be used, depending on whether access is requested to non-secure or secure web sites. Claim 1 of Applicants' invention, as now amended, reads as follows:

> A method of secure session management and authentication between a web site and a web client, said web site having secure and non-secure web pages, said method comprising the steps of:
>
> utilizing a non-secure communication protocol and a session cookie when said web client requests access to said non-secure web pages; and
>
> utilizing a secure communication protocol and creating an authcode cookie when said web client requests access to said secure web pages, so that utilizations of said authcode cookie are interspersed between utilizations of said session cookie;
>
> using said authcode only for allowing said web client to access secure web pages; and
>
> following creation of said authcode cookie, using said session cookie to access specified non-secure web pages, without first requiring use of said authcode cookie in order to access said specified non-secure web pages.

A prior art reference anticipates a claimed invention under 35 U.S.C. § 102 only if every element of the claimed invention is identically shown in that

single reference, arranged as they are in the claims. *In re Bond*, 910 F. 2d 831, 832, 15 U.S.P.Q. 2d 1566, 1567 (Fed Cir. 19990). All limitations of the claimed invention must be considered when determining patentability. *In re Lowry*, 32 F. 3d 1579, 1582, 21 U.S.P.Q. 2d 1031, 1034 (Fed Cir. 1994). Anticipaton focuses on whether a claim reads on the product or process a prior art reference discloses, not on what the reference broadly teaches. Kalman v. Kimberly-Clark Corp., 713 F. 2d 760, 218 U.S.P.Q. 781 (Fed Cir. 1983).

The pertinent teaching of the Koneru reference is set forth in the abstract thereof, which reads as follows:

> A system and method is disclosed for tracking a user across both secure and non-secure areas on an Internet and/or Internet site. In one aspect of the system and method, when a user first accesses a non-secure area, such as a public area, the user is assigned a token, such as a globally-unique identifier (GUID). The token is used as a key to a database entry on a server computer for tracking the user in non-secure areas. When the user first accesses a secure area, the user is prompted to enter a user identification and a password. The user identification is then used as a key to the database entry, rather than the token. The server then uses the user identification to track the user across both secure and non-secure areas. (Emphasis added.)

This teaching is further emphasized in the Koneru specification, such as at column 6, lines 55-61, and at Claim 1, which respectively read as follows:

> Using the present invention, the method of tracking a user depends upon whether the user has accessed a secure area 78. Prior to accessing a secure area 78, the server 58 tracks the user based upon the GUID stored in the client identifier on the client computer 20. After the user has accessed the secure area 78, the system tracks the user based upon a user identifier entered by the user. (Emphasis added.)

> 1. A method of tracking a user on a client computer as the user accesses secure and non-secure areas on a network server computer, comprising the steps of:
> upon first accessing a non-secure area, assigning a token representing the user wherein the token does not contain a user identification and using the token as a key for accessing a database entry associated with the user on the server computer;

> upon first accessing the secure area, receiving a user identifier associated with the user;
> after accessing the secured area, replacing the token with the user identification as the key to the database entry; and
> the database entry including customization information associated with user. (Emphasis added.)

From the above statements set forth in the Koneru reference, it is abundantly clear that when the user first accesses a non-secure area on a server, the user is assigned a token, or a GUID. The token is used as an access key for non-secure areas only until the first time that the user accesses a secure area. Thereupon, the token is replaced with a user identification. From then on, the user identification is used as the access key for both secure and non-secure areas. (Koneru Abstract; Claim 1, col. 9, lines 1-2).

The above principle, that the user identification is the access key for both secure and non-secure areas, is further emphasized in Koneru at Figure 5, and at col. 8, lines 6-36 pertaining thereto. Figure 5 shows both a non-secure area 76 and a secure area 78. Process block 110 teaches that access to both the secure and non-secure areas requires use of the user identification.

To the extent that there is any equivalency or correspondence between Applicants' Claim 1 and the Koneru disclosure, the session cookie of Claim 1 would correspond to the token or GUID of Koneru, and the authcode cookie of Claim 1 would correspond to the user identification of Koneru. In view of this, Applicants respectfully submit that Koneru does not teach every element of Claim 1, arranged as they are therein. Specifically, Koneru does not teach the following features or limitations now recited by Claim 1, in the combination thereof:

> (1) The authcode cookie is used only to allow the web client to access secure web pages.
> (2) Following creation of the authcode cookie, the session cookie is used to access a specified non-secure web page, without first requiring use of the authcode cookie to access the non-secure web page.

(3) A non-secure protocol, as well as session cookie, are utilized when accessing a non-secure web site.

Applicants' feature (1), referred to above, is essential for Applicants' purpose. In contrast, Koneru emphasizes repeatedly that the user identification is to be used to access non-secure areas, as well as secure areas. In addition to Koneru sections referred to above, this is explicitly taught in Koneru at col. 2, lines 60-62. As stated therein, "using the user identification as a key, only one database entry is needed to track users across both non-secure and secure areas." Moreover, as discussed above in connection with Figure 5 of Koneru, this figure teaches that non-secure area 76 cannot be accessed without using the user identification. Accordingly, the disclosure of Koneru clearly teaches away from the Claim 1 requirement that an authcode cookie, provided to access secure web pages, must be used only to allow the web client to access secure web pages.

With regard to feature (2) of Applicants' Claim 1, Figure 5 of Koneru appears to show that public and private areas of non-secure area 76 are accessed using the GUID of Koneru. This is apparently done to provide "a heightened level of authentication", as taught at col. 8, lines 31-32. However, Figure 5 of Koneru shows very clearly that before the GUID can be used to access a non-secure area, data base entry must first be provided by the user identification. This is taught by process block 110 of Figure 5, which states that "Server uses the user identification to access a database entry." (Emphasis added.) Moreover, this teaching of Koneru is reinforced at col. 7, lines 57-59. Therein, it is stated that "Process block 98 shows that the server no longer uses the GUID as the key to data entry. Instead, the GUID is replaced as the key with the user identification". (Emphasis added.) These teachings of Koneru clearly direct away from the Claim 1 recitation of using the session cookie to access a specified non-secure web page, without first requiring use of an authcode cookie, that has been provided only to access secure web pages.

In regard to the above-referenced protocol, Applicants have carefully reviewed the Koneru et al. reference, including col. 2, lines 12-27 thereof. However, Applicants have been unable to find any particular reference or teaching therein regarding non-secure communication protocol, or to the

utilization thereof when a web client requests access to non-secure web pages, as is recited by Applicants' Claim 1.

Applicants consider that the cited Rieche reference fails, either alone or in any combination with the Koneru et al. reference, to overcome the deficiencies of Koneru discussed above in regard to amended Claim 1.

IV. Response to Rejection of Remaining Claims

Claim 12 is considered to distinguish over the art, including the Koneru et al. and Reiche references, particularly in reciting that the authcode is for allowing web client access only to secure web pages. This clearly distinguishes over the Koneru teachings, for reasons given in support for feature (1) of Applicants' Claim 1.

Independent Claim 20 is considered to distinguish over the art, including both the Koneru et al. and Reiche references, for reasons given in support of Claims 1 and 12.

Claims 2-11 respectively depend from Claim 1, and are each considered to distinguish over the art for the same reasons given in support thereof.

Claims 13-19 respectively depend from Claim 12, and are each considered to distinguish over the art for the same reasons given in support thereof.

Claims 21-31 and 33 respectively depend from Claim 20, are each considered to distinguish over the art for the same reasons given in support thereof.

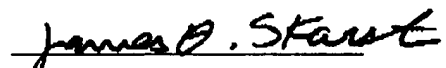
CONCLUSION

It is respectfully urged that the subject application is patentable over the Kaneru et al. and Reiche references, and is now in condition for allowance.

The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: April 15, 2005

Respectfully submitted,



James O. Skarsten
Reg. No. 28,346
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Attorney for Applicants